What you need to know about

USB Storage Devices

protecting your information

By Master Sgt. Josh Walker
AFCA Information Systems Security Policy

SCOTT AFB, Ill. —As with any new technology, there are risks associated with usage, and USB storage devices are no exception.

USB storage devices can easily introduce viruses into a computer network. Anti-virus filters and firewalls are installed to protect and defend today's computer networks against viruses. However, using USB storage devices bypasses those security mechanisms because they plug directly into a computer potentially allowing a new virus or worm to spread across the entire network. Because USB storage capabilities are so massive, there's also the potential of bringing in other dangerous and unauthorized software including shareware, freeware and spyware.

The second major risk in using USB storage devices is data loss or theft. Any unattended USB storage device or any unlocked computer with a USB port becomes a rich source of sensitive information. The thief could be anyone, making the insider threat that much more dangerous. A person may simply lose the device since it's so small. If someone finds it, they may return it but what if it fell into the wrong hands? If someone simply borrows your USB storage device and returns it to you, will it now have a virus?

Using USB storage devices in a classified environment presents other risks. Because most of these devices don't have write protection mechanisms, placing a USB storage device into a classified computer makes it classified at the same level as the system. **There's currently no approved utility to sanitize flash memory.** Once classified, you must use the storage device only in classified environments or, when no longer needed, destroy it. Many organizations do not wish to accept the risks of using USB storage devices in classified environments and have prohibited their use.

Becoming aware of the risks with using these devices is a great beginning to safeguarding information. Air Force Instructions does not specifically mention USB storage devices, but they are a form of portable/removable media and therefore subject to all Air Force policies regarding media. This includes, but is not limited to AFI 33-202, Network and Computer Security, and Air Force Systems Security Instruction 5020, Remanence Security.

To prevent someone from downloading information to a USB storage device, ensure the system has a password-protected screen saver enabled and remove common access cards from readers before leaving the computer unattended. Ensure the use of antivirus software, keep it up-to-date and use it. Scan all removable media, including USB storage devices, for viruses before each use. Some USB storage devices come with additional security features like password protection, encryption and biometrics.

Before buying one, find out if your organization has a policy on approved USB storage devices. Ensure the media is marked and labeled IAW AFI 31-401, Information Security Program Management. Marking and labeling will help control media during loss and prevent inadvertent use of unclassified USB storage devices in classified computers. USB storage devices are portable, handy and have incredible storage capabilities. They also have a few security challenges. Unfortunately, there is no single magic spell to counter the risks presented by them. Awareness of the risks is the best method of protecting information or, in other words, keep the genie in the bottle and the power in the palm of your hand.

Portable Universal Serial Bus storage devices are, essentially, flash memory drives (sometimes called thumb or pen drives) capable of storing 1Mb to 5GB of information. Compatible with just about any computer with a USB port, files can transfer at a rate of 1Mb per second without a separate power supply or battery. It can be reused more than one million times and preserved for more than 10 years.